Department of Homeland Security Daily Open Source Infrastructure Report for 19 January 2006

Current Nationwide Threat Level is ELEVATED — Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- The Arizona Republic reports one of three reactors at the Palo Verde nuclear power plant was shut down Tuesday, January 17, after operator Arizona Public Service Co. discovered a problem with the unit's main emergency shut−down line. (See item 1)
- The U.S. Department of Agriculture has announced additional efforts in collaboration with states and private industry to protect the nation's food supply from terrorist threats. (See item 23)
- US−CERT has released Technical Cyber Security Alert TA06−018A: Oracle products contain multiple vulnerabilities. (See item 31)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *January 18, Arizona Republic* — **Palo Verde shuts down a nuclear reactor.** One of three reactors at the Palo Verde nuclear power plant was shut down Tuesday, January 17, after operator Arizona Public Service Co. (APS) discovered a problem with the unit's main emergency shut−down line. APS has monitored the problem closely for years but it became more pronounced when the Phoenix−based utility restarted Unit 1 the week before Christmas

after a refueling and repair outage. Unit 1's emergency shut−down line experienced an "acoustic impact" that vibrated the reactor's shut−down line beyond acceptable levels. APS had been operating the reactor at one−third of capacity due to the vibrations, but operators decided to shut down the reactor and attempt to fix the problem. According to APS spokesperson Jim McDonald the unit could restart within two days. Potential fixes could include adding shock absorbers, installing weights, or adding heat to the emergency shut−down line. A contributing factor to the vibrations could be the unit's new twin, 800−ton steam generators and turbines which APS recently replaced in the unit's largest construction job since the reactor opened in 1986. Palo Verde, located 50 miles west of downtown Phoenix, is the nation's largest nuclear power plant and a critical source of power for the Southwest and the Valley.
Source: http://www.azcentral.com/business/articles/0118paloverde18.h tml

2. *January 18, The Huntsville Times (AL)* — **Seal leaks force shutdown of Browns Ferry reactor.** One of the two operating reactors at Browns Ferry nuclear plant near Athens, AL, was shut down Sunday, January 15, after a seal problem was discovered on the pumps that push water through the reactor to generate steam. The reactor was shut down manually around 12:30 p.m. CST Sunday, said Craig Beasley, spokesperson for Browns Ferry. The recirculation pumps, which draw water from the bottom of the reactor and run it through pumps into the middle of the reactor, will have leaking seals replaced, Beasley said. The repair work on the pumps is sometimes done during planned reactor shutdowns, he said, but this shutdown followed indications that the pump seals were leaking more than usual. Ken Clark, an Atlanta−based spokesperson for the Nuclear Regulatory Commission, said the pumps act essentially as a reactor coolant system. He said initial reports indicate there was no damage to the pumps, only the seals. Beasley said the Tennessee Valley Authority (TVA) "typically does not give away downtime schedules" and he provided no time estimate for repair. TVA has two operating reactors at Browns Ferry and is working to rebuild Unit 1, which it hopes to return to operations next year.
Source: http://www.al.com/news/huntsvilletimes/index.ssf?/base/news/113757947411150.xml&coll=1

3. *January 17, Bloomberg* — **Gasoline prices may return to $3 record as U.S. demand rebounds.** Gasoline pump prices may return to $3 a gallon in the U.S. this summer as demand recovers and conservation efforts in the aftermath of Hurricanes Katrina and Rita prove to be temporary. Gasoline consumption last month touched an all−time high, equal to an average of 21.6 million barrels a day in the four weeks ending Friday, December 30, according to government data, signaling the hurricanes' effects didn't last. Katrina in August and Rita in September disrupted 29 percent of U.S. refining, and the national average pump price jumped to a record $3.069 a gallon. Gasoline prices are likely to average $2.41 a gallon in 2006, according to Energy Department analysts in Washington. Even with the rally after Katrina last year, the U.S. pump price average over 12 months was $2.27 a gallon. Prices dropped to about $2.20 a gallon in December, lower than before the storms. The price of crude oil, which is the largest part of retail gasoline's cost, may rise again this year as global economic growth spurs demand.
Source: http://www.bloomberg.com/apps/news?pid=10000087&sid=a4yqakPx VvrM

4. *January 17, Reuters* — **China, U.S. to boost world oil demand growth.** A rebound in Chinese demand growth and stronger U.S. consumption will drive up world oil demand in 2006, the

International Energy Agency (IEA) said on Tuesday, January 17, increasing the strain on the Organization of the Petroleum Exporting Countries (OPEC) spare capacity. The IEA, adviser to 26 industrialized nations, forecast demand would grow at 2.2 percent in 2006, up from 1.3 percent growth in 2005. At 1.8 million bpd, the IEA's figures on 2006 global demand growth were unchanged from its last monthly report. On paper, new oil coming onstream this year from inside and outside OPEC should more than meet the predicted rise in demand. But oil markets are rising on concern about lost production in Nigeria and a threat to Iranian output as well as doubts promised new oil will materialize. This year, the IEA is cautiously predicting an acceleration in non−OPEC supply of 1.3 million bpd, while new OPEC oil should provide a further one million bpd. But the IEA noted current OPEC spare capacity of less than 1.5 million bpd was "below comfort levels." IEA also stated "...while spare capacity is expected to build this year, there is some statistical uncertainty."
Source: http://news.yahoo.com/s/nm/20060117/bs_nm/energy_iea_dc_4

5. *January 17, Associated Press* — **Wyoming sets coal output record as prices rise.** Despite logistics problems last year, it appears Wyoming continues to produce record amounts of coal, which is the subject of increasing national demand and fetching strong prices. Coal industry analysts at the U.S. Department of Energy's Energy Information Administration estimate the actual figure for 2005 is about 407.2 million tons, with the additional tonnage coming from Powder River Basin operations. Last year also saw a dramatic price increase in Wyoming coal. "It's just amazing what's going on in the industry right now. I don't think it's fully appreciated how much utilities are willing to pay for coal right now," said Paul Klibanow, a coal industry analyst for the New York investment firm Force Capital Management. A combination of coal train derailments, disruption in natural gas supplies on the Gulf Coast, and skyrocketing prices for emission credits worked together in 2005 to jolt coal prices upward. Now, spot market prices for Powder River Basin coal of 8,800 British thermal units is $22 per ton. Since the derailments prevented basin producers from meeting all the increased customer demand in 2005, utility inventories are at record lows, and they are desperately trying to replenish their coal stockpiles.
Source: http://www.billingsgazette.com/index.php?id=1&display=rednews/2006/01/17/build/wyoming/40−coal−output.inc

[Return to top]

Chemical Industry and Hazardous Materials Sector

6. *January 18, Philadelphia Inquirer* — **Tanker spill snarls interstate traffic in Pennsylvania.** The fifty−five gallons of xylene that splashed onto Interstate−95 in South Philadelphia, PA, early Tuesday, January 17, from an overturned tanker closed a one−mile stretch of the highway the entire day, and well into the evening. The incident occurred on the interstate between Packer Avenue and South Broad Street. The spill occurred around 5:30 a.m. EST, when a southbound tanker truck hopped a 29−inch concrete center barrier and overturned. The truck came to rest in the northbound lanes, officials said. The tanker contained 6,400 gallons of xylene, a volatile solvent most often used in the rubber, printing and leather industries. Only a small fraction of the chemical escaped from the dome of the tanker, said Daniel Williams, executive chief of the Philadelphia Fire Department. But even that much was cause for alarm. One spark might have set off a disastrous fire that could have blown up the nearly full tanker.

The highway was completely shut down until 7:45 p.m. EST, when the southbound lanes were cleared. The northbound side was reopened about a half hour later.
Source: http://www.philly.com/mld/philly/news/13649021.htm

[Return to top]

Defense Industrial Base Sector

7. *January 18, GovExec* — **Lawmakers urge Navy to boost submarine orders.** Rep. Rob Simmons (R−CT) has urged the Navy to double its annual orders for Virginia−class nuclear submarines earlier than planned, a move that would help keep afloat a struggling sector of the defense industry and protect potentially thousands of jobs. In a letter late last week to Chief of Naval Operations Adm. Michael Mullen, Simmons and other congressional supporters of the submarine program implored the Navy to boost production on the nuclear−powered vessels to two ships a year beginning in fiscal 2009, three years earlier than the Navy has planned. The lawmakers argued that the Navy's slow procurement plan will hinder efforts to realize Mullen's goal of maintaining a fleet of 48 nuclear−powered submarines. The Navy now has 54 submarines, many of which will be retired over the next several years. Under the Navy's current schedule, the submarine force would bottom out at 40 boats in 2028. Starting to build two subs a year in fiscal 2009 instead of fiscal 2012 would bring the number to 43. Simmons added that producing two boats a year would help bring overall costs on the $2.4 billion submarines down to the Navy's $2 billion goal.
Source: http://www.govexec.com/story_page.cfm?articleid=33189&dcn=to daysnews

8. *January 18, Global Security Newswire* — **Defense review to focus on handling of irregular threats.** The forthcoming U.S. Quadrennial Defense Review will focus heavily on confronting weapons of mass destruction and terrorism threats through work with allies and new technological capabilities, a top Department of Defense official said Wednesday, January 18. The department’s work on the review, which is an extension of the March 2005 National Defense Strategy, centered on providing the president and military commanders with more options for handling “asymmetric” threats, U.S. Principal Defense Undersecretary for Policy Ryan Henry said. The Monday, February 6, review, said Henry, will call on the department to reorient capabilities toward threats that are “irregular,” “catastrophic” or “disruptive” in nature, and away from the “traditional” threats toward which current capabilities are overly directed. “We need to provide them [combatant commanders] more capabilities to guarantee effects,” Henry said. “We don’t know how we’re going to use the force in the future, and so we have to have a capabilities set that will span all reasonable futures.” Offering one example of the new capabilities being discussed, Henry said the Pentagon in the future would "continue to emphasize a robust nuclear capability" but will also rely more on other weapons to support nuclear deterrence.
Source: http://www.nti.org/d_newswire/issues/2006_1_17.html#272D64FF

[Return to top]

Banking and Finance Sector

9. *January 18, Washington Post* — **Selling stampede shuts down Tokyo stock market.** A stampede of sell orders forced the shut−down of the world's second−biggest stock exchange on Wednesday, January 18, as investors fled the Tokyo market, spooked by fall−out from an investigation into Internet company Livedoor. The Tokyo Stock Exchange suspended trading 20 minutes before the normal closing time after the number of trades threatened to exceed its computer system's capacity of 4.5 million per day. It the first time that the exchange was forced to halt trading as a result of capacity constraints since it opened in 1949. Livedoor was raided by prosecutors on Monday, January 16, for suspicion of fudging financial reports and spreading false information to boost its share price. News of the raid extended a sell−off that has wiped out more than $300 billion in shareholder value −− about equal to the gross domestic product of Sweden −− in just three days. The exchange has been hit by a series of recent system problems. Hideo Ueki, chief investment officer at UBS Global Asset Management Japan said "...this problem will likely add to the growing negative sentiment in the market. I'm pretty sure the NYSE has only had to shut down for snow or a black−out."
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/01/18/AR2006011800180_pf.html

10. *January 17, News Tribune (WA)* — **Computer forensics lab cracks down on identity theft.** Pierce County, WA, is attacking identity theft with new technology that could warn potential victims sooner and lock up thieves longer. A computer forensics lab will allow them to dig deeper into the hardware and software Pierce County law enforcement officers seize as part of identity theft cases. Bill Garrison, who supervises the investigative services unit of the prosecutor's office, said "(We'll find) hundreds if not thousands of victims in waiting who don't even know their names have been compromised." As an early example of what the new lab can offer, investigators have discovered 1,384 area residents whose identities were stolen from a local tax preparation service. Their names, addresses, Social Security numbers, and employers' names were part of the files discovered on a computer connected to a suspect in the case. That computer also had software to create counterfeit checks and credit cards. "We know that [identity theft] is the crime of the future," sheriff's spokesperson Ed Troyer said. The new computers allow investigators to delve into any type of computer hard drive, cellular phone, or other media. The added evidence could bring more serious charges, including allegations related to organized crime, and lengthier prison terms against identity thieves.
Source: http://www.thenewstribune.com/news/local/story/5463122p−4929 726c.html

11. *January 17, Associated Press* — **New Yorkers being told about ID security breaches.** More than 200,000 New York residents have already received potentially bad news under a new state law about the security of their personal information. The law that took effect Wednesday, December 7, requires companies and government agencies to notify consumers whenever a report containing their telephone numbers, bank account information, income, medical records, and other information is accidentally disseminated. In just five weeks, 200,541 state residents have gotten such notices from 10 companies and government offices, said Marc Violette, spokesperson for Attorney General Eliot Spitzer. Tom Conway, head of consumer fraud and protection bureau for the state attorney general's office, said so far there have not been any instances similar to last year's ChoicePoint Inc. case in which thieves posing as small business customers gained access to its data base and possibly compromised the personal information of 145,000 people. There were about 50 million security breaches nationwide in 2005. Legislation on security breach notification was enacted in at least 22 states in 2005, according to the

National Conference of State Legislatures.
Source: http://www.buffalonews.com/editorial/20060117/1010747.asp

12. *January 17, Finextra* — **HSBC cash machines fitted with tracking devices.** HSBC, a United Kingdom bank, is attaching satellite tracking devices to its ATMs in a bid to stop units being stolen. HSBC is fitting some cash machines with tracking devices and putting up signs next to bugged machines in an effort to deter thieves, who steal bulldozers in order to remove through−the−wall ATMs and then drive off with them. The device is being attached to an unspecified number of machines located at vulnerable sites. A HSBC spokesperson said that the satellite tracking technology is one of many anti−fraud measures implemented by the bank. But the spokesperson declined to say how many units have been fitted with the device or how many ATMs had already been stolen. In a more low−tech response to a spate of bulldozer attacks on its ATMs in 2004, Bank of Ireland thwarted thieves by simply emptying machines of their cash after branch closing times.
Source: http://finextra.com/fullstory.asp?id=14762

13. *January 16, South Bend Tribune (IN)* — **Obituaries linked to fraud ring.** Between July and October 2005, a prisoner used The South Bend Tribune newspaper's obituary section in a fraud scheme involving at least 47 people. Sgt. Dominic Zultanski of the South Bend, IN, Police Department said the organized group used obituaries to find names and track them down with listed phone numbers. A prisoner used the facility's phone to make a collect call to an accomplice, who made a three−way call with the victim. The inmate claimed to be from the Social Security Administration, a credit card company, bank, or credit bureau, Zultanski said. After expressing sorrow for the widow's loss, the inmate persuaded the victim to give him personal information, such as credit card information. In 2002, two other inmates allegedly used obituaries from The Tribune and possibly other newspapers to execute the scheme with smuggled cell phones, Zultanski said. They charged more than $70,000 on the credit cards, Stewart said. The schemers established trust with their victims because they knew all Visa card numbers begin with "4," MasterCard numbers begin with "5" and Discover card numbers begin with "6011." Visa and MasterCard, which issue cards to banks, also have bank identification numbers bearing the same first six digits.
Source: http://www.southbendtribune.com/apps/pbcs.dll/article?AID=/20060116/News01/601160318/0/SPORTS

[Return to top]

Transportation and Border Security Sector

14. *January 18, New York Sun* — **L line becomes New York's first computer−controlled train.** New York's first computer−controlled train carrying passengers rolled out of the Rockaway Parkway station early Monday morning, January 16, Metropolitan Transit Authority (MTA) officials said. The MTA activated the long−awaited Communication−Based Train Control system on two trains on a stretch of seven stops along the L line in Brooklyn, a spokesperson for the authority, Charles Seaton, said. Transit officials are quietly testing the technology on trains with few actual passengers. The trains are under the computer's influence between Rockaway Parkway and Broadway Junction. Tests are scheduled to take place from midnight to 5 a.m. EST every night this week. The motorman, who ordinarily has sole discretion over the

train, has no decision−making responsibilities. The motorman still drives the train, but he takes all his orders from the computer, including how fast to go and when to slow to a stop. The next phase of the system's development will remove the motorman's driving responsibilities altogether. When implemented, an off−train computer will control all the trains operating on the L line by radio. A motorman will still ride the train to control the doors and tell the computer when it is safe to leave the station.
Source: http://www.nysun.com/article/26068

15. *January 18, Associated Press* — **Guns, non−explosive device found in car at U.S.−Canada border.** Four handguns and what Royal Canadian Mounted Police (RCMP) thought was "possibly a pipe bomb" were found Tuesday night, January 17, in a car that had just entered Canada at the Peace Arch border crossing. The firearms −− a 9 mm handgun, two shotguns, and a rifle with a rifle stock −− were found in an initial inspection of the car and the device, which turned out to be not explosive, was found in the engine compartment, according to a statement posed on the RCMP's Website. The device "had some wires protruding from it and was suspicious in nature," but the Mounties' explosives squad determined that it did not contain explosives, according to the statement signed by RCMP Cpl. Roger Morrow. "It appears as though the male is suffering from a mental illness," Morrow said in the statement. "It is expected the individual will be returned to the border crossing, turned over to Canadian Immigration who in turn will ensure the safe return of the gentleman to the United States." Border officers checked the car after it entered Canada because the driver was acting erratically, Shore said.
Source: http://seattletimes.nwsource.com/html/localnews/2002747250_w ebborder18.html

16. *January 18, Asbury Park Press (NJ)* — **Ferry is escorted to safety after taking on water.** The U.S. Coast Guard and New York Police escorted a NY Waterway ferry to safety in Manhattan after it left the Belford terminal in Middletown and began to take on water during the storm on Wednesday, January 18. Passenger William McBride, a 38−year−old stock trader from Sea Bright, said the boat that left Belford around 7:30 a.m. EST, was being tossed about like a cork, and passengers were turning green. "From almost the start the boat was in terrible situation," he said. "The water was up to our ankles. People were making...calls home, telling their wives they might be in the water." The U.S. Coast Guard's New York Station received reports that the ferry, named the Peter Weiss, was taking on water over its side near the Verrazzano−Narrows Bridge at 7:56 a.m. Tom Beckendorff, the master of the ferry, ordered the 149 passengers to put on life jackets as a safety precaution, according to a Coast Guard news release. The Coast Guard and police met the boat near the bridge, and escorted it to Pier 11. According to the NY Waterway Website, service from Belford, Port Liberte, and Liberty Harbor is suspended until further notice because of the weather.
Source: http://www.app.com/apps/pbcs.dll/article?AID=/20060118/NEWS/ 60118012

17. *January 18, Department of Transportation* — **Secretary Mineta announces tunnel−boring machine start.** Construction of a new light rail tunnel under parts of Seattle, WA, began Wednesday, January 18, thanks in part to $244.15 million in New Starts transit funding provided by the Department of Transportation's Federal Transit Administration (FTA), Transportation Secretary Mineta announced. The tunnel boring work is part of Sound Transit's Central Link Light Rail $2.44 billion transit project. The Beacon Hill station will be excavated to a depth of 180 feet and the actual tunnels will be excavated using a state−of−the−art

tunnel−boring machine to bore twin tunnels about one−mile long. FTA Project Management Consultants and Sound Transit are closely following the contractor's progress, safety plans, and quality assurance procedures due to the sophisticated nature of the work. Considered a vital cornerstone of Seattle's transportation future, the project is part of a regional transportation program that includes light and commuter rail and express bus service for three counties.
Source: http://www.dot.gov/affairs/fta0106.htm

[Return to top]

Postal and Shipping Sector

18. *January 18, North County Times (CA)* — **Veteran San Diego city employee pleads innocent to theft charges.** A city public works employee accused of using her work computer to gain personal information on customers, as well as stealing mail from post office boxes, pleaded innocent Tuesday, January 17, to 36 criminal charges. Jacqueline Annette Lawrence, a 16−year employee of San Diego's General Services Department, was ordered held on $200,000 bail. She faces 13 felony counts of using stolen personal identification to defraud and 23 misdemeanor counts for allegedly having someone else's personal identifying information and planning to use it to defraud someone. Deputy District Attorney Joan Stein also alleged that Lawrence, 48, stole mail from boxes at a Chula Vista post office and used personal identifying information to make credit card purchases. Many pieces of stolen mail were found during a search of the defendant's apartment. Lawrence's arrest was carried out by the U.S. Postal Inspection Service and the Computer and Technology Hi−Tech Response Team, a multi−agency task force.
Source: http://www.nctimes.com/articles/2006/01/18/news/sandiego/17_40_121_17_06.txt

[Return to top]

Agriculture Sector

19. *January 18, Max Planck Society (Germany)* — **New possibilities to fight pests with biological means.** Max Planck Society researchers in Jena, Germany, have identified a gene which produces a chemical "cry for help" that attracts beneficial insects to damaged plants, including corn. Corn plants emit a cocktail of scents when they are attacked by certain pests, such as a caterpillar known as the Egyptian cotton leaf worm. Parasitic wasps use these plant scents to localize the caterpillar and deposit their eggs on it, so that their offspring can feed on the caterpillar. Soon after, the caterpillar dies and the plant is relieved from its attacker. In the case of corn, only one gene, TPS10, has to be activated to attract the parasitic wasps. This gene carries information for a terpene synthase, an enzyme forming the sesquiterpene scent compounds that are released by the plant and attract wasps toward the damaged corn plant. Since this mechanism is based only on a single gene, it might be useful for the development of crop plants with a better resistance to pests.
Source: http://www.mpg.de/english/illustrationsDocumentation/documentation/pressReleases/2006/pressRelease200601171/index.html

20. *January 18, Indiana AgConnection* — **Purdue improves Website for National Biosecurity Resource Center.** The National Biosecurity Resource Center for Animal Health Emergencies'

new and improved Website is up and running. The Website continues to house the truck wash database for the National Pork Board's Truck Quality Assurance Program, state regulations for carcass disposal and state regulations for reporting of animal diseases. New on the Website is a searchable database for information on disinfectants. The new Website also will house educational programs and informational papers on current issues in animal health. Another feature is a secure, password−protected, Web−based tool for collection, storage and management of resource information important to respond to an animal emergency. Provisions are being made for Web−based data entry by local authorities and voluntary data entry by local citizenry. The community resource information will only be available to select local authorities and will not be available to the general public. The center is a cooperative effort between the Purdue Homeland Security Institute of Discovery Park, the Purdue University School of Veterinary Medicine and the Indiana Board of Animal Health. Its mission is to provide information and tools to enable government, commodity groups, veterinarians, producers and the public to meet the challenges of animal health emergencies.
National Biosecurity Resource Center: http://www.biosecuritycenter.org/
Source: http://www.indianaagconnection.com/story−state.cfm?Id=32&yr= 2006

21. *January 18, Kentucky AgConnection* — **New organization formed to manage animal ID.** A new organization to manage animal identification information was unveiled last week. The United States Animal Identification Organization (USAIO) held its first board meeting Tuesday, January 10, to elect members of the board, said chairman Charles Miller, a cow−calf producer from Nicholasville, KY. The formation of the USAIO was spearheaded by the National Cattleman's Beef Association. The board will be expanded as other industry groups adopt the USAIO as the database for animal movement data needed for the National Animal Identification System (NAIS), Miller said. "This organization looks forward to working closely with industry and animal health authorities to move the NAIS forward in a positive, proactive way," he said. "USAIO looks forward to engaging all the interested parties to provide an effective, efficient, and inexpensive database for the NAIS." The USAIO has submitted a Memorandum of Understanding to the U.S. Department of Agriculture to form a strategic partnership for sharing database information, Miller said.
Source: http://www.kentuckyagconnection.com/story−state.cfm?Id=28&yr =2006

22. *January 17, StopSoyBeanRust* — **Nine Florida counties positive for rust on kudzu last week.** A team of soybean rust experts found soybean rust active on kudzu in nine counties in central and northern Florida last week, including one county that did not have soybean rust in 2005. The counties were reported positive as of Tuesday, January 17, on the U.S. Department of Agriculture soybean rust site. Scott Isard, Glen Hartman and four graduate students from the University of Illinois and Penn State University drove two vehicles for 2,500 miles around Florida from Wednesday, January 11, to Friday, January 13, according to Tuesday's updated state commentary by James Marois, University of Florida plant pathologist. The team's intensive scouting resulted in positive finds of soybean rust in nine Florida counties: Polk, Duval, Leon, Alachua, Pasco, Hernando, Hillsborough, Lee and Gadsden. Polk county was the only one of the nine counties with no soybean rust finds in 2005. Up until these finds, soybean rust on kudzu in Montgomery County, AL, was the first and only reported U.S. find in 2006. Now there are 10 counties positive for soybean rust in the United States this year. Rust was found in 138 counties in 2005.
Florida state commentary on soybean rust: http://www.sbrusa.net/

Source: http://www.stopsoybeanrust.com/viewStory.asp?StoryID=672

[Return to top]

Food Sector

23. *January 17, U.S. Department of Agriculture* — **U.S. Department of Agriculture continues efforts to safeguard the nation's food supply.** The U.S. Department of Agriculture (USDA) Tuesday, January 17, announced additional efforts in collaboration with states and private industry to protect the nation's food supply from terrorist threats. USDA's Food Safety and Inspection Service (FSIS) will conduct five critical food defense exercises this year. The first exercise will take place in Alameda, CA, on Wednesday, January 18, and Thursday, January 19. These exercises are designed to practice reporting a non−routine incident while coordinating with all levels of government, non−governmental agencies and the private sector in an incident command system structure. These exercises will challenge all participants to collaborate more closely and become better prepared to keep the food supply safe. The first day of the exercise will focus on non−routine incident reporting and how program offices would manage an emergency and the second day will focus on product recall and public health and communication issues. Additionally, FSIS will test its ability to coordinate with organizations outside of USDA, such as the local and state departments of health and agriculture.
Additional information about agrosecurity can be found on USDA's Website: http://www.usda.gov/homelandsecurity/
Source: http://www.usda.gov/wps/portal/!ut/p/_s.7_0_A/7_0_1OB?contentidonly=true&contentid=2006/01/0010.xml

24. *January 16, Food Production Daily* — **Funding directed at new foods and processing techniques in the European Union.** Designated food "clusters" in the European Union (EU) will receive a boost in funding to help the bloc's researchers develop innovative foods and processing techniques. The Commission also announced a series of new projects under a program to increase research and development in the food sector. The funding is part of a European Commission policy to encourage more research into new foods and processing techniques. Low spending on research and development by the EU's food industry has been identified as a drawback to the sector's competitiveness. Some of the new funding money from the European Commission will fund a two−year project investigating how best to increase food innovation within the EU and drive competitiveness. The newly−created Food Innovation Network Europe (FINE) will target Europe's "food clusters". These are East Netherlands, Scotland, Flanders (Belgium), Rogaland (Norway), Wielkopolska (Poland), Emilia−Romagna (Italy), Castilla León (Spain) and Oresund (Denmark and Sweden). Funding has also been directed at integrating research by veterinary, medical, and food scientists' research on the prevention and control of zoonoses, including food borne diseases. A project called Cascade will research the effects of chemical residues on human health.
Source: http://www.foodproductiondaily.com/news/ng.asp?n=65109−r−d−s afety−network

[Return to top]

Water Sector

25. *January 18, Southwest Farm Press* — **Drought conditions persist across Southwest region.** The National Oceanic and Atmospheric Administration (NOAA) lists most of East Texas, from west of Dallas to the Louisiana state line and south to near College Station, in “extreme drought,” going up to six months without appreciable rainfall. Stock tanks are either dry or falling fast. Fall−planted wheat has either not germinated or has gotten just enough rain to poke through the soil and then wither in dry, windy conditions. Wildfires have destroyed rangeland, landscapes, and homes and have accounted for several fatalities in Texas. Data from NOAA indicates conditions across most of the South as being very dry. Extreme drought conditions extend into Oklahoma with most of the state either extreme or severe. The western edge of Oklahoma is listed as near normal, as is the Texas Panhandle and most of New Mexico. Source: http://southwestfarmpress.com/news/060118−drought−persist−re gion/

26. *January 16, MetroWestDailyNews (MA)* — **New treatment plan to help address Massachusetts water concerns.** The Massachusetts Department of Environmental Protection (DEP) is putting its foot down. After sending Wayland five notices in the past 18 months for not complying with state water regulations, the DEP has sent the town a consent order of stricter requirements. If Wayland does not adhere to the new requirements, the state will fine the town $5,225, with additional fines for each day the town is in violation. Under the new guidelines, the town will be required to speciate −− or break down −− any positive coliform samples collected this year to better determine where the bacteria is coming from. The town will also have to collect heterotrophic plate counts (HPC) on a monthly basis. Like the speciation tests, HPC collections break down bacteria. The Water Department already takes these collections from water leading into the distribution system; now it will collect from the distribution system as well, said David Fields, the department’s working foreman. These requirements come after the most serious of Wayland’s recent water violations. In October, the town reported four coliform positive samples, one of which tested positive for E. coli. The town failed to notify the public of the E. coli discovery within 24 hours, as required by the state. Source: http://www.metrowestdailynews.com/localRegional/view.bg?arti cleid=119459

[Return to top]

Public Health Sector

27. *January 18, World Health Organization* — **Information sharing paramount in comprehensive avian flu pandemic planning.** On Wednesday, January 18, at the International Pledging Conference on Avian and Human Influenza in Beijing, World Health Organization (WHO) Director−General Dr. Lee Jong−wook underscored the areas requiring urgent international and national action to fight avian influenza and prepare for a pandemic. Jong−wook acknowledged that most countries have comprehensive plans and that vigilance, surveillance, and information sharing are paramount. For example, Turkey's open sharing of virus samples with researchers is resulting in unique information about the virus. Keeping populations informed is also vital, he said. Communities need to understand what to do, and why, in the event of an outbreak. Countries that do not yet have endemic H5N1, must know what to look for. Rapid and thorough investigation of new cases in Indonesia has provided new clues about exposure risks. China's outbreaks showed how political commitment at the highest level allows even the largest countries to scale up surveillance and response systems.

Cambodia's experience showed that weak basic infrastructures restrict data collection and prevent the decisive action that comes from a clear picture. Jong−wook said that there must be visible improvement in control of avian influenza and pandemic preparedness by countries, technical agencies, and all others involved.
Source: http://www.who.int/dg/lee/speeches/2006/flumeeting_beijing/e n/index.html

28. *January 18, Reuters* — **Brazil's Rio de Janeiro fears dengue epidemic as cases rise.** An outbreak of dengue fever in Brazil's tourist Mecca of Rio de Janeiro has prompted authorities to increase prevention measures, fearing a repeat of a 2002 epidemic that killed more than 100 people. "We have flare−ups in two districts. It needs to be blocked urgently, because without such control we have a risk of having an epidemic again in Rio," said Aloisio Ribeiro, head of Rio state government's Epidemiology Vigilance Center. Dengue is carried by mosquitoes and causes severe body pain, fever, and headaches. State and municipal authorities will launch a task force on Thursday, January 19, to combat the disease with vehicle−mounted insecticide sprayers and inspections of private homes. December's total number of cases was three times higher than a year earlier. Rio is preparing to receive hundreds of thousands of tourists for its Carnival in February. "The problem is that there are plenty of mosquitoes, that Rio is an endemic area, and there has not been enough effort to prevent dengue," Ribeiro said. Because the disease is common within the region, its residents are more likely to contract more than one of dengue's four strains, increasing the chance of a potentially deadly hemorrhagic form of the disease.
Source: http://health.yahoo.com/news/143223

29. *January 17, Reuters* — **Inventor develops anti−malaria wristwatch.** A South African inventor has developed an anti−malaria wristwatch to help combat one of Africa's biggest killers by monitoring the blood of those who wear it and sounding an alarm when the parasite is detected. Gervan Lubbe said his "Malaria Monitor" wristwatch, due to launch next month, could save lives and keep millions out of hospital by heading off the disease before patients even feel ill. "It picks up the parasite and destroys it so early that the possibility of dying is absolutely zero and you don't even feel the early cold symptoms," Lubbe said. Malaria kills more than one million people every year and makes 300 million seriously ill, according to the World Health Organization. Ninety percent of deaths are in sub−Saharan Africa. The digital timepiece pricks the wrist with a tiny needle four times a day and tests the blood for malaria parasites. If the parasite count tops 50 an alarm sounds and a brightly−colored picture of a mosquito flashes on the watch face. The wearer must take three tablets that kill the disease within 48 hours. He has received 1.5 million orders for the wristwatch from companies, governments, and aid organizations working in Africa.
Source: http://health.yahoo.com/news/143198

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

30. *January 01, CSO Magazine* — **Lessons learned from Hurricane Katrina.** Experts have been weighing lessons learned from Hurricane Katrina. U.S. Coast Guard Vice Adm. Thad Allen is principal federal official for the Gulf Coast recovery from Hurricane Katrina. In a recent interview, Allen said the episode should serve as a real−world drill for a premeditated attack. So, what did we learn from the drill? Are we prepared for such an attack? "I don't think the national response plan anticipated how we would react to what I'd call a catastrophic loss of the elements of a civil society," Allen says. "New Orleans was taken down hard. This is far beyond the scale for what might have been envisioned for a natural disaster response and comes closer to what you might envision if a weapon of mass effect was used on a municipality. From that standpoint the lessons learned from this will be extremely useful."
Source: http://www.csoonline.com/read/010106/katrina_cleanup.html

[Return to top]

Information Technology and Telecommunications Sector

31. *January 18, US−CERT* — **Technical Cyber Security Alert TA06−018A: Oracle products contain multiple vulnerabilities.** Oracle has released a critical patch update that addresses more than eighty vulnerabilities in different Oracle products and components. The impact of these vulnerabilities varies depending on the product, component, and configuration of the system. Potential consequences include the execution of arbitrary code or commands, information disclosure, and denial of service. Vulnerable components are likely to be available to attackers via remote networks and with limited or no prior authorization. An attacker who compromises an Oracle database may be able to gain access to sensitive information. According to Oracle, three of the vulnerabilities corrected un the Oracle Critical Patch Update for January 2006 affect Oracle Database Client−only installations. US−CERT recommends that sites running Oracle review the Critical Patch Update, apply patches, and take other mitigating action as appropriate.
US−CERT is tracking all of these issues under VU#545804:
http://www.kb.cert.org/vuls/id/545804
Oracle Critical Patch Update − January 2006:
http://www.oracle.com/technology/deploy/security/pdf/cpujan2 006.html
Source: http://www.us−cert.gov/cas/techalerts/TA06−018A.html

32. *January 18, Financial Times* — **Hackers blackmail Website.** The FBI is investigating the hijacking of a Website that hosts micro−advertisements by hackers who demanded a ransom to restore the site. Alex Tew of Britain was sent a demand for US$50,000 by e−mail by a hacker, believed to be Russian. When he refused, the Website crashed. Tew first received a threat on January 7 from a body calling itself The Dark Group, demanding $5,000. He thought the blackmail was a hoax and took little notice. However, on Wednesday, January 18, when Tew reached his goal of earning $1 million, the hackers intensified their attack and hijacked the Website.
Source: http://news.ft.com/cms/s/cd05a42c−87c6−11da−8762−0000779e234 0.html

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT is aware of a public exploit for a vulnerability in VERITAS NetBackup Volume Manager Daemon (vmd). The VERITAS NetBackup vmd listens on network port 13701/tcp. An attacker could send a specially crafted packet to the Volume Manager on a vulnerable system to cause a buffer overflow or a denial of service condition. Successful exploitation may allow may allow a remote, unauthenticated attacker to execute arbitrary code on a vulnerable system with root or SYSTEM privileges. More information about this vulnerability can be found in the following URL:

VU#574662 VERITAS NetBackup library buffer overflow vulnerability:
http://www.kb.cert.org/vuls/id/574662

US−CERT strongly encourages users and administrators to review the following mitigation to address this vulnerability as soon as possible:

Review the Symantec Advisory SYM05−024 and apply the recommended updates to address this vulnerability:

http://seer.support.veritas.com/docs/279553.htm

http://support.veritas.com/menu_ddProduct_NBUESVR_view_DOWNL OAD.htm

Restrict access to the ports used by the NetBackup services.

Malicious Website Exploiting Sun Java Plug−in Vulnerability US−CERT is aware of an active malicious website that exploits a vulnerability in the Sun Java JRE. The initial report led US−CERT to believe the website was exploiting VU#974188. After further analysis, it was determined that the actual vulnerability being exploited was VU#760344. This vulnerability allows a Java Applet to bypass java security settings. Once these checks are bypassed, a remote attacker may be able to exploit this vulnerability to execute arbitrary code on the host machine. More information about these vulnerabilities can be found in the following URL:

VU#760344 Sun Java Plug−in fails to restrict access to private Java packages:
http://www.kb.cert.org/vuls/id/760344

VU#974188 Sun Java Runtime Environment "reflection" API privilege elevation vulnerabilities: http://www.kb.cert.org/vuls/id/974188

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 6881 (bittorrent), 445 (microsoft−ds), 25 (smtp), 139 (netbios−ssn), 6346 (gnutella−svc), 32801 (−−−), 50497 (−−−), 80 (www), 27015 (halflife) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

Nothing to report.

[Return to top]

General Sector

Nothing to report.

[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer